PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059358
(43)Date of publication of application : 25.02.2000

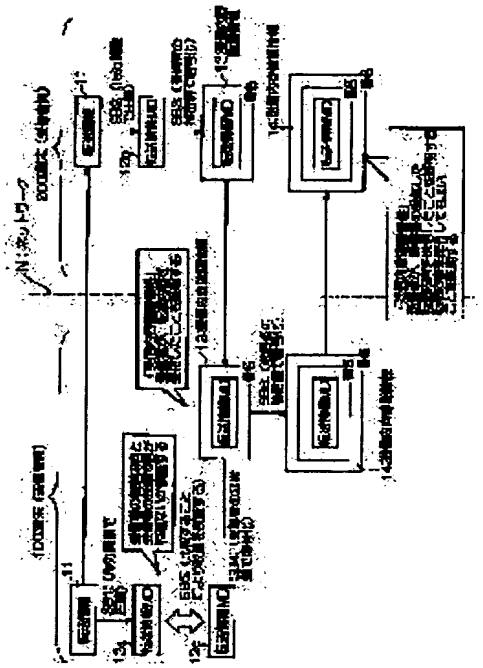
(51)Int.CI. H04L 9/32
G09C 1/00
H04L 1/16
H04L 29/08

(21)Application number : 10-227410
(22)Date of filing : 11.08.1998

(71)Applicant : MITSUBISHI MATERIALS CORP
(72)Inventor : OKUBO TATSUMASA
TOYODA SHOICHI

(54) INFORMATION FALSIFICATION DETECTOR AND COMPUTER READABLE RECORDING MEDIUM STORING FALSIFICATION DETECTION PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain the information falsification detector that detects falsifica tion of information and a computer readable recording medium that storing a falsification detection program by even in the case of a terminal without a right of decoding received information.
SOLUTION: A system has a terminal 100 and a terminal 200 connecting to the terminal 100 via a network N, and the terminal 100 uses a hash function to compress transfer information 11 and to generate transfer information MD 12a. The terminal 100 transmits the transfer information 11 to the terminal 200 via the network N. After receiving the transfer information 11, the terminal 200 uses a hash function to compress the transfer information 11 and generates transfer information MD12b and encrypts the transfer information MD12b and uses a private key of a recipient to encrypt the transfer information MD12b to generate reception contents confirmation information 13. The terminal 100 compares transfer information MD12c with transfer information MD12b to certify whether or not falsification is made.



LEGAL STATUS

[Date of request for examination] 31.03.2000
[Date of sending the examiner's decision of rejection] 26.08.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－59358
（P2000－59358A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04L	9/32		H04L	9/00	675B　5K013
G09C	1/00	640	G09C	1/00	640D　5K014
					640B　5K034
H04L	1/16		H04L	1/16	
	29/08			13/00	307Z

審査請求　未請求　請求項の数23　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－227410

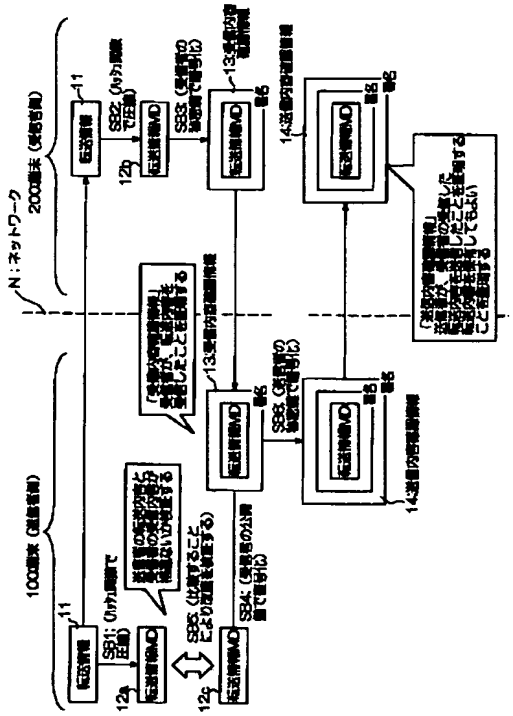
(22)出願日　平成10年８月11日(1998.8.11)

(71)出願人　000006264
三菱マテリアル株式会社
東京都千代田区大手町１丁目５番１号
(72)発明者　大久保　達真
埼玉県大宮市北袋町１丁目297番地　三菱マテリアル株式会社総合研究所内
(72)発明者　豊田　祥一
埼玉県大宮市北袋町１丁目297番地　三菱マテリアル株式会社総合研究所内
(74)代理人　100064908
弁理士　志賀　正武　（外９名）

Ｆターム(参考)　5K013 AA08 GA03 GA07 GA08 JA00
5K014 AA01 BA00 EA01 HA00
5K034 AA05 DD01 FF01 HH02 HH09

(54)【発明の名称】　情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体を得ること。
【解決手段】　本発明は端末１００と端末１００にネットワークＮを介して接続された端末２００とを有しており、端末１００は、ハッシュ関数を用いて転送情報１１を圧縮して、転送情報ＭＤ１２ａを作成する。端末１００は、転送情報１１をネットワークＮを介して端末２００へ送信する。端末２００は、転送情報１１を受信した後、ハッシュ関数を用いて転送情報１１を圧縮して、転送情報ＭＤ１２ｂを作成した後、受信者の秘密鍵を利用して転送情報ＭＤ１２ｂを暗号化して、受信内容確認情報１３を生成する。端末１００は、転送情報ＭＤ１２ｃと転送情報ＭＤ１２ａとを比較することにより、改竄が行われたか否かを検証する。



1

【特許請求の範囲】

【請求項１】　送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、

前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、

前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、

前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、

前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項２】　前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に基づいて前記受信内容確認情報を作成することを特徴とする請求項１に記載の情報改竄検知装置。

【請求項３】　前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記受信内容確認情報を作成することを特徴とする請求項１に記載の情報改竄検知装置。

【請求項４】　前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に対して電子署名したものを前記受信内容確認情報として作成することを特徴とする請求項１に記載の情報改竄検知装置。

【請求項５】　前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報を作成し、

該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものを作成し、

前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものを前記受信内容確認情報として作成することを特徴とする請求項１に記載の情報改竄検知装置。

2

【請求項６】　送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、

前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、

前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、

前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、

前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７】　受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、

前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成された受信内容確認情報を前記ネットワークを介して受信する受信手段と、

前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項８】　前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報であることを特徴とする請求項７に記載の情報改竄検知装置。

【請求項９】　前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする請求項７に記載の情報改竄検知装置。

【請求項１０】　前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に対して電子署名したものであることを特徴とする請求項７に記載の情報改竄検知装置。

【請求項１１】　前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に基づいて作成され、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものに基づいて作成され、
前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものであることを特徴とする請求項７に記載の情報改竄検知装置。

【請求項１２】　受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、
前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成され、受信内容確認情報を前記ネットワークを介して受信する受信手段と、
前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１３】　送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、
前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、
前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、
前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、
前記受信内容確認情報に基づいて、送信者側端末が、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を作成し、前記ネットワークを介して前記受信側端末へ送信する送信内容確認情報作成手段と、
前記送信内容確認情報作成手段から送信された前記送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項１４】　前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報に基づいて前記送信内容確認情報を作成することを特徴とする請求項１３に記載の情報改竄検知装置。

【請求項１５】　前記送信内容確認情報作成手段は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記送信内容確認情報を作成することを特徴とする請求項１３記載の情報改竄検知装置。

【請求項１６】　前記送信内容確認情報作成手段は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成することを特徴とする請求項１３に記載の情報改竄検知装置。

【請求項１７】　前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストを前記送信内容確認情報として作成し、
前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成し、
前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものに基づいて前記送信内容確認情報を作成することを特徴とする請求項１３に記載の情報改竄検知装置。

【請求項１８】　送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、
前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、
前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、
前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容

確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項１９】　前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報であることを特徴とする請求項１８に記載の情報改竄検知装置。

【請求項２０】　前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする請求項１８に記載の情報改竄検知装置。

【請求項２１】　前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものであることを特徴とする請求項１８に記載の情報改竄検知装置。

【請求項２２】　前記送信内容確認情報は、
前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて作成され、
前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものに基づいて作成され、
前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものであること、
を特徴とする請求項１８に記載の情報改竄検知装置。

【請求項２３】　送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、
前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、
前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、
前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、ネットワーク伝送における情報改竄の検知に用いられる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】従来、情報の改竄を検知する技術（以下、情報改竄検知技術と称する）としては、電子署名技術が情報改竄検知装置により実用化されている。一般的な電子署名技術の例としては、Digital Signature Algorithmや公開鍵暗号方式（例えばＲＳＡ方式）とハッシュ関数（例えば、ＭＤ２）と組み合わせるものがある。

【０００３】図７は、上述した従来の情報改竄検知装置の動作原理を説明する図である。図７に示す情報改竄検知装置は、送信者側に設置された送信端末１と、該送信端末１と図示しないネットワーク（インターネット等）を介して接続され、受信者側に設置された受信端末６とから概略構成されている。この情報改竄検知装置において、暗号化、復号化には、公開鍵および秘密鍵が用いられる。この公開鍵と秘密鍵とは、秘密鍵から公開鍵が計算により求めることができる一方、逆に公開鍵から秘密鍵が計算により求めることができないという関係とされている。

【０００４】上記構成において、ステップＳＡ１では、送信端末１は、受信端末６へ送信すべき平文２を暗号化する。具体的には、送信端末１は、受信者（受信端末６）の公開鍵を利用して平文２から暗号文３を作成する。次いで、ステップＳＡ２では、送信端末１は、ハッシュ関数を用いて平文２を圧縮して、ＭＤ（メッセージダイジェスト）４ａを作成する。

【０００５】ここで、ハッシュ関数とは、同じ出力値になる任意の２つの異なる入力を発見することが計算量的に実行不可能な関数をいい、電子署名等のメカニズムの一部として利用する目的で、長いメッセージから比較的短い一定値長の圧縮データをハッシュ符号として作成するための一方向関数をいう。次に、ステップＳＡ３では、送信端末１は、送信者（送信端末１）の秘密鍵を利用してＭＤ４ａから認証子５を作成する。この認証子５は、暗号文３のもとになる平文２に対してされた電子署名である。ここでは、電子署名は、メッセージダイジェストの作成という第１プロセス、該メッセージダイジェストに対する秘密鍵による暗号化という第２プロセスを経てなされるものである。また、電子署名は、上記プロセスの他にメッセージダイジェスト化されていない情報、またはメッセージダイジェストと該情報とを組み合わせたものに対する秘密鍵による暗号化というプロセスを経てなされる場合も含む。

【０００６】そして、送信端末１は、上記暗号文３および認証子５をネットワークを介して、受信端末６へ送信する。これにより、受信端末６は、暗号文３および認証

子５を受信した後、まず、ステップＳＡ４で受信者（受信端末６）の秘密鍵を利用して暗号文３を復号化して、平文２を作成する。次いで、ステップＳＡ５では、受信端末６は、ハッシュ関数を用いて復号化された平文２を圧縮することにより、ＭＤ４ｂを作成する。

【０００７】また、ステップＳＡ６では、受信端末６は、受信された認証子５を送信者（送信端末１）の公開鍵を利用することにより復号化して、ＭＤ４ｃを作成する。そして、ステップＳＡ７では、受信端末６は、ＭＤ４ｂとＭＤ４ｃとを比較することにより、転送情報（暗号文３および認証子５）に改竄が行われたか否かの改竄検証を行う。ここで、ＭＤ４ｂとＭＤ４ｃとが一致している場合には、転送情報に対して改竄が行われていないことを意味する一方、両者が不一致である場合には、転送情報に対して改竄が行われていることを意味する。

【０００８】

【発明が解決しようとする課題】ところで、従来の情報改竄検知装置においては、図７に示すように、受信した暗号文３を復号化する権利を有する受信端末６では、転送（送信）途中で転送情報に対して改竄が行われたか否かを、ＭＤ４ｂとＭＤ４ｃとの比較結果から検知することができる。

【０００９】しかしながら、従来の情報改竄検知装置においては、図８に示すように受信した暗号文３を復号化する権利を有しない、言い換えれば、受信者の秘密鍵を有しない受信端末６では、平文２ひいてはＭＤ４ｂを作成することができないため、転送情報に対する改竄検証を行うことができないという欠点があった。

【００１０】したがって、従来の情報改竄検知装置においては、図８に示す受信端末６が更に図示しない別の端末へ転送情報を転送した場合、該端末は、たとえ、暗号文３を復号化する権利を有していても、改竄がいつどこで行われたかを検知することができない。さらに、従来の情報改竄検知装置においては、最初に転送情報を転送する送信端末１がもとの平文２より作成された認証子５（電子署名）でない電子署名を転送した場合であっても、上記端末が改竄を検知することができない。つまり、従来の情報改竄検知装置においては、重要な転送情報に対して改竄が行われた場合、改竄が行われた端末（場所）、時間の特定が重要になるが、これらの検知・特定を行うことができないのである。

【００１１】本発明はこのような背景の下になされたもので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１２】

【課題を解決するための手段】請求項１に記載の発明は、送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項２に記載の発明は、請求項１に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に基づいて前記受信内容確認情報を作成することを特徴とする。また、請求項３に記載の発明は、請求項１に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記受信内容確認情報を作成することを特徴とする。また、請求項４に記載の発明は、請求項１に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に対して電子署名したものを前記受信内容確認情報として作成することを特徴とする。また、請求項５に記載の発明は、請求項１に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報を作成し、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものを作成し、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものを前記受信内容確認情報として作成することを特徴とする。また、請求項

６に記載の発明は、送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体である。また、請求項７に記載の発明は、受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成された受信内容確認情報を前記ネットワークを介して受信する受信手段と、前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項８に記載の発明は、請求項７に記載の情報改竄検知装置において、前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報であることを特徴とする。また、請求項９に記載の発明は、請求項７に記載の情報改竄検知装置において、前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする。また、請求項１０に記載の発明は、請求項７に記載の情報改竄検知装置において、前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に対して電子署名したものであることを特徴とする。また、請求項１１に記載の発明は、請求項７に記載の情報改竄検知装置において、前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか１つ、または複数組み合わせた情報に基づいて作成され、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものに基づいて作成され、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものであることを特徴とする。また、請求項１２に記載の発明は、受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成され、受信内容確認情報を前記ネットワークを介して受信する受信手段と、前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体である。また、請求項１３に記載の発明は、送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記受信内容確認情報に基づいて、送信者側端末が、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を作成し、前記ネットワークを介して前記受信側端末へ送信する送信内容確認情報作成手段と、前記送信内容確認情報作成手段から送信された前記送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項１４に記載の発明は、請求項１３に記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報に基づいて前記送信内容確認情報を作成することを特徴とする。また、請求項１５に記載の発明は、請求項１３記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記

受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記送信内容確認情報を作成することを特徴とする。また、請求項１６に記載の発明は、請求項１３に記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成することを特徴とする。また、請求項１７に記載の発明は、請求項１３に記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストを前記送信内容確認情報として作成し、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成し、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものに基づいて前記送信内容確認情報を作成することを特徴とする。また、請求項１８に記載の発明は、送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項１９に記載の発明は、請求項１８に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報であることを特徴とする。また、請求項２０に記載の発明は、請求項１８に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする。また、請求項２１に記載の発明は、請求項１８に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものであることを特徴とする。また、請求項２２に記載の発明は、請求項１８に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか１つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて作成され、前記受信内容確認情報と前記確認情報のうちいずれか１つ、または複数組み合わせた情報に対して電子署名したものに基づいて作成され、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか２つ以上の情報を組み合わせたものであることを特徴とする。また、請求項２３に記載の発明は、送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００１３】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。図１は本発明の一実施形態による情報改竄検知装置の動作原理を説明する図である。この図に示す情報改竄検知装置は、送信者側に設置された端末１００と、該端末１００にインターネット等のネットワークＮを介して接続された端末２００とから概略構成されている。

【００１４】上記構成において、ステップＳＢ１では、端末１００は、ハッシュ関数を用いて転送情報１１を圧縮して、転送情報ＭＤ（メッセージダイジェスト）１２ａを作成する。この転送情報ＭＤ１２ａは、後述するように送信者の転送内容と受信者の受信内容とが相違していないか否かの検証に用いられる。次いで、端末１００は、上記転送情報１１をネットワークＮを介して端末２００へ送信（転送）する。

【００１５】これにより、端末２００は、転送情報１１を受信した後、ステップＳＢ２で、ハッシュ関数を用いて転送情報１１を圧縮して、転送情報ＭＤ１２ｂを作成する。ここで、転送情報１１に対する改竄が行われていない場合、上記転送情報ＭＤ１２ｂと転送情報ＭＤ１２

ａとは、同一である。一方、改竄が行われた場合、転送情報ＭＤ１２ｂと転送情報ＭＤ１２ａとは、異なる。

【００１６】そして、ステップＳＢ３では、端末２００は、受信者（端末２００）の秘密鍵を利用して転送情報ＭＤ１２ｂを暗号化して、受信内容確認情報１３を生成する。この受信内容確認情報１３は、転送情報ＭＤ１２ｂに対して受信者（端末２００）による電子署名が行われたものであり、受信者（端末２００）が転送内容（転送情報１１）を受信したことを証明する情報である。ここでは、電子署名は、メッセージダイジェスト化、暗号化という２つのプロセスを経てなされたものである。また、電子署名は、上記プロセスの他にメッセージダイジェスト化されていない情報、またはメッセージダイジェストと該情報とを組み合わせたものに対する秘密鍵による暗号化というプロセスを経てなされる場合も含む。要は電子署名は、圧縮されている、いないに関わらずある情報に対して秘密鍵により暗号化されたものである。次いで、端末２００は、上記受信内容確認情報１３をネットワークＮを介して端末１００へ送信する。

【００１７】これにより、端末１００は、上記受信内容確認情報１３を受信した後、ステップＳＢ４で、受信者（端末２００）の公開鍵により受信内容確認情報１３を復号化して、転送情報ＭＤ１２ｃを作成する。次に、ステップＳＢ５では、端末１００は、転送情報ＭＤ１２ｃと転送情報ＭＤ１２ａとを比較することにより、改竄が行われたか否かを検証する。具体的には、端末１００は、転送情報ＭＤ１２ａと転送情報ＭＤ１２ｃとが同一である場合、検証結果を未改竄とする一方、転送情報ＭＤ１２ａと転送情報ＭＤ１２ｃとが異なる場合、検証結果を改竄とする。

【００１８】次に、ステップＳＢ６では、端末１００は、送信者（端末１００）の秘密鍵を利用して受信内容確認情報１３を暗号化して、送信内容確認情報１４を作成する。この送信内容確認情報１４は、受信内容確認情報１３に対して送信者（端末１００）による電子署名が行われたものであり、送信者（端末１００）が、受信者（端末２００）の受信した転送内容（転送情報１１）を送信したことを証明するための情報である。また、送信内容確認情報１４は、受信者（端末２００）が転送内容（転送情報１１）を保有してもよいことを証明するための情報である。

【００１９】図２は、本発明の一実施形態による情報改竄検知装置の具体的な構成を示すブロック図である。この図において、図１の各部に対応する部分には同一の符号を付ける。図２に示す端末１００において、１０１は、転送情報１１をネットワークＮを介して端末２００へ送信する情報送信部である。１０２は、端末２００から送信される受信内容確認情報１３（図１参照）をネットワークＮを介して受信する情報受信部である。

【００２０】１０３は、図１に示すステップＳＢ１、ＳＢ４およびＳＢ５の処理を実行する受信内容確認情報確認部であり、メッセージダイジェスト作成部１０３ａ、送信者・通信・受信者情報取得部１０３ｂおよび電子署名確認部１０３ｃとを有している。受信内容確認情報確認部１０３において、メッセージダイジェスト作成部１０３ａは、図１に示すステップＳＢ１の処理を実行するものであり、転送情報１１をハッシュ関数で圧縮して転送情報ＭＤ１２ａを作成する。送信者・通信・受信者情報取得部１０３ｂは、転送情報１１、受信内容確認情報１３から各送信者情報、通信情報、受信者情報を取得する。

【００２１】ここで、送信者情報は、送信者（端末１００）に関する情報であり、「送信者名」、「ＩＤ」、「公開鍵ＩＤ」、「メールアドレス」、信頼性が高い第三者機関によって発行された「電子証明書」等の情報である。また、通信情報は、端末１００と端末２００との間の通信に関する情報であり、「通信時間」、「受信時間」、「通信方式」、「通信ＩＤ」等の情報である。また、受信者情報は、受信者（端末２００）に関する情報であり、「受信者名」、「ＩＤ」、「公開鍵ＩＤ」、「メールアドレス」、信頼性が高い第三者機関によって発行された「電子証明書」等の情報である。図２に示す電子署名確認部１０３ｃは、受信内容確認情報１３（図１参照）の電子署名が受信者（端末２００）によるものであるかを確認する。

【００２２】１０４は、図１に示すステップＳＢ６等の処理を実行する送信内容確認情報作成部であり、メッセージダイジェスト作成部１０４ａ、送信者・通信・受信者情報取得部１０４ｂおよびメッセージダイジェスト作成部１０４ａとを有している。この送信内容確認情報作成部１０４は、受信内容確認情報１３に基づいて、送信内容確認情報１４を作成する。

【００２３】この送信内容確認情報作成部１０４において、メッセージダイジェスト作成部１０４ａは、受信内容確認情報１３からメッセージダイジェストを作成する。送信者・通信・受信者情報取得部１０４ｂは、上述した送信者・通信・受信者情報取得部１０３ｂと同様にして、受信内容確認情報１３から送信者情報、通信情報および受信者情報を取得する。電子署名付加部１０４ｃは、受信内容確認情報１３を送信者（端末１００）の秘密鍵により暗号化することにより、受信内容確認情報１３に対して（電子）署名を付加する。１０５は、ネットワークＮを介して送信内容確認情報１４を端末２００へ送信する情報送信部である。

【００２４】一方、端末２００において、２０１は、端末１００からネットワークＮを介して送信される転送情報１１を受信する情報受信部である。２０２は、図１に示すステップＳＢ２およびＳＢ３の処理を実行する受信内容確認情報作成部であり、メッセージダイジェスト作成部２０２ａ、送信者・通信・受信者情報取得部２０２

ｂおよび電子署名付加部２０２ｃとを有している。この受信内容確認情報作成部２０２は、転送情報１１に基づいて受信内容確認情報１３を作成する。

【００２５】この受信内容確認情報作成部２０２において、メッセージダイジェスト作成部２０２ａは、転送情報１１をハッシュ関数で圧縮することにより、転送情報ＭＤ１２ｂ（図１参照）を作成する。送信者・通信・受信者情報取得部２０２ｂは、上述した送信者・通信・受信者情報取得部１０３ｂと同様にして、転送情報１１に関する送信者情報、通信情報および受信者情報を取得する。電子署名付加部２０２ｃは、転送情報ＭＤ１２ｂ（図１参照）を受信者（端末２００）の秘密鍵により暗号化することにより、転送情報ＭＤ１２ｂに対して（電子）署名を付加する。ここで、この署名が付加された転送情報ＭＤ１２ｂは、受信内容確認情報１３である。

【００２６】また、２０５は、端末１００から送信された送信内容確認情報１４の内容を転送情報１１に基づいて確認する送信内容確認情報確認部であり、メッセージダイジェスト作成・取得部２０５ａと、送信者・通信・受信者情報取得部２０５ｂと、電子署名確認部２０５ｃとを有している。この送信内容確認情報確認部２０５において、メッセージダイジェスト作成・取得部２０５ａは、上述したメッセージダイジェストを作成する機能と、受信内容確認情報作成部２０２のメッセージダイジェスト作成部２０２ａによりすでに作成された転送情報ＭＤ１２ｂ（図１参照）を取得する機能とを有する。ここで、上記転送情報ＭＤ１２ｂを取得した場合には、メッセージダイジェスト作成・取得部２０５ａは、メッセージダイジェストを作成しない。送信者・通信・受信者情報取得部２０５ｂは、上述した送信者・通信・受信者情報取得部１０３ｂと同様にして、送信者情報、通信情報および受信者情報を取得する。電子署名確認部２０５ｃは、送信者（端末１００）の公開鍵を用いて、受信内容確認情報１３に対する署名を確認する。

【００２７】次に、上述した一実施形態による情報改竄検知装置の動作について図３～図６に示すフローチャートを参照しつつ説明する。図３は、図２に示す受信内容確認情報確認部１０３の動作を説明するフローチャートであり、図４は、図２に示す送信内容確認情報作成部１０４の動作を説明するフローチャートである。また、図５は、図２に示す受信内容確認情報作成部２０２の動作を説明するフローチャートであり、図６は、図２に示す送信内容確認情報確認部２０５の動作を説明するフローチャートである。

【００２８】図２において、端末１００における転送情報１１が情報送信部１０１によりネットワークＮを介して端末２００へ送信されると、該転送情報１１は、端末２００の情報受信部２０１により受信される。これにより、端末２００の受信内容確認情報作成部２０２は、図５に示すフローチャートに従って受信内容確認情報１３を生成する。

【００２９】具体的には、図５に示すステップＳＥ１では、受信内容確認情報作成部２０２は、受信内容（転送情報１１）を入力する。これにより、ステップＳＥ２では、メッセージダイジェスト作成部２０２ａは、受信内容（転送情報１１）をハッシュ関数で圧縮してメッセージダイジェスト（図１：転送情報ＭＤ１２ｂ）を作成する。なお、図５に示す例では、ステップＳＥ２の処理を実行することなく、ステップＳＥ１からステップＳＥ６へ進んでもよい。

【００３０】また、ステップＳＥ３～ＳＥ５では、受信内容確認情報作成部２０２は、送信者情報（送信者名、ＩＤ、公開鍵ＩＤ、メールアドレス、電子証明書等）、受信者情報（受信者名、ＩＤ、公開鍵ＩＤ、メールアドレス、電子証明書等）、通信情報（送信時間、受信時間、通信方式、通信ＩＤ等）を転送情報１１から取り込む。

【００３１】これにより、ステップＳＥ６では、送信者・通信・受信者情報取得部２０２ｂは、ステップＳＥ３～ＳＥ５で入力された送信者情報、受信者情報および通信情報を取得した受信内容確認情報作成部２０２は、上述した受信内容（転送情報１１）と、 転送情報ＭＤ１２ｂ、送信者情報、受信者情報、通信情報等の各情報とを統合する。ここで、情報の統合とは、ハッシュ関数で圧縮された転送情報ＭＤ１２ｂの全部または一部と、送信者情報における送信者名、ＩＤ等、受信者情報における受信者名、ＩＤ等、通信情報における送信時間、受信時間等のうち１つまたは複数の情報とを組み合わせることをいう。

【００３２】次に、ステップＳＥ７では、メッセージダイジェスト作成部２０２ａは、ステップＳＥ６で統合された情報をハッシュ関数で圧縮することにより、メッセージダイジェストを作成する。次いで、ステップＳＥ８では、電子署名付加部２０２ｃは、ステップＳＥ７で作成されたメッセージダイジェストを受信者の秘密鍵で暗号化することにより、メッセージダイジェストに対して、電子署名を付加する。そして、ステップＳＥ９では、受信内容確認情報作成部２０２は、各情報を統合化することにより、図１に示す受信内容確認情報１３を作成した後、これを情報送信部２０３へ出力する。また、メッセージダイジェスト作成部２０２ａは、必要に応じて転送情報ＭＤ１２ｂを送信内容確認情報確認部２０５のメッセージダイジェスト作成・取得部２０５ａへ出力する。この場合、メッセージダイジェスト作成・取得部２０５ａは、メッセージダイジェストの作成を行うことなく、上記転送情報ＭＤ１２ｂを取得する。

【００３３】そして、上記受信内容確認情報１３は、情報送信部２０３によりネットワークＮを介して端末１００へ送信された後、端末１００の情報受信部１０２により受信される。これにより、端末１００の受信内容確認

情報確認部１０３は、図３に示すフローチャートに従って、受信内容確認情報１３の内容を確認することにより、改竄を検知する。

【００３４】具体的には、図３に示すステップＳＣ１では、受信内容確認情報確認部１０３は、情報受信部１０２により受信された受信内容確認情報１３を入力した後、ステップＳＣ２へ進む。ステップＳＣ２では、メッセージダイジェスト作成部１０３ａは、受信者の公開鍵を用いて受信内容確認情報１３を復号化することにより、メッセージダイジェスト（図１：転送情報ＭＤ１２ｃ）を作成（取得）する。

【００３５】そして、ステップＳＣ３では、電子署名確認部１０３ｃは、受信者（端末２００）の公開鍵を用いて、受信内容確認情報１３が受信者により署名されたものであるか否かを確認する。ここで、受信内容確認情報１３が受信者（端末２００）の公開鍵で復号化できた場合、受信内容確認情報１３は、受信者により署名されたものであり、一方、受信内容確認情報１３が受信者の公開鍵で復号化できなかった場合、受信内容確認情報１３は受信者により署名されなかったものである。

【００３６】次に、ステップＳＣ４では、受信内容確認情報確認部１０３は、ステップＳＣ３の確認結果から、受信内容確認情報１３の署名が受信者（端末２００）の署名であるか否かを判断し、同判断結果が「ＮＯ」の場合、改竄もしくは通信エラーが発生したものとする。一方、ステップＳＣ４の判断結果が「ＹＥＳ」の場合、受信内容確認情報確認部１０３は、ステップＳＣ５へ進む。

【００３７】ステップＳＣ５では、受信内容確認情報１３に含まれている各種情報を分類する。ここで、上記各種情報としては、受信情報内容、前述した送信者情報、受信者情報、通信情報、メッセージダイジェスト（転送情報ＭＤ１２ｃ）等がある。

【００３８】また、受信内容確認情報確認部１０３は、ステップＳＣ６へ進み、転送情報１１、送信者が転送した、通信に関する送信者情報、通信情報、受信者情報等を入力する。次に、ステップＳＣ７では、受信内容確認情報確認部１０３のメッセージダイジェスト作成部１０３ａは、転送情報１１をハッシュ関数で圧縮して転送情報ＭＤ１２ａ（図１参照）を作成する。

【００３９】そして、受信内容確認情報確認部１０３は、ステップＳＣ９～ＳＣ１２で受信内容と送信内容とを比較することにより、受信内容の検証を情報毎に行う。そして、ステップＳＣ１３では、受信内容確認情報確認部１０３は、上記ステップＳＣ９～ＳＣ１２の検証結果を受けて、受信内容が送信内容と相違ないか否かを判断し、同判断結果が「ＮＯ」の場合、改竄もしくは通信エラーが発生しているものとする。一方、受信内容確認情報確認部１０３は、受信内容が送信内容と相違していない場合、ＳＣ１３の判断結果を「ＹＥＳ」として、改竄が発生していないものとする。

【００４０】次いで、送信内容確認情報作成部１０４は、図４に示すフローチャートに従って、送信内容確認情報１４（図１参照）を作成する処理を実行する。すなわち、送信内容確認情報作成部１０４は、図４に示すステップＳＤ１で受信内容確認情報１３を入力した後、ステップＳＤ２で受信内容確認情報承認情報を生成する。ここで、受信内容確認情報承認情報とは、受信内容確認情報確認部１０３が受信内容確認情報１３の内容を承認（確認）した旨を示す情報である。この承認（確認）した旨を示す情報は、承認した時間、端末、承認者（一実施形態では送信者）に関する情報を元に生成される。

【００４１】次いで、ステップＳＤ３では、送信内容確認情報作成部１０４は、受信内容確認情報１３と受信内容確認情報承認情報とを統合する。次に、ステップＳＤ４では、メッセージダイジェスト作成部１０４ａは、ステップＳＤ３において統合された情報のメッセージダイジェストを取得した後、ステップＳＤ５へ進む。ステップＳＤ５では、電子署名付加部１０４ｃは、送信者（端末１００）の秘密鍵により暗号化することにより、メッセージダイジェストに対して署名を行う。

【００４２】そして、ステップＳＤ６では、送信内容確認情報作成部１０４は、ステップＳＤ３における各種情報とステップＳＤ５において署名されたメッセージダイジェストとを統合化する。これにより、送信内容確認情報作成部１０４においては、送信内容確認情報１４が作成され、該送信内容確認情報１４は、情報送信部１０５へ出力される。

【００４３】そして、上記送信内容確認情報１４は、情報送信部１０５により、ネットワークＮを介して端末２００へ送信された後、端末２００の情報受信部２０４により受信される。

【００４４】これにより、端末２００の送信内容確認情報確認部２０５は、図６に示すフローチャートに従って、送信内容確認情報１４の確認を実行する。具体的には、図６に示すステップＳＦ１では、送信内容確認情報確認部２０５は、情報受信部２０４により受信された送信内容確認情報１４を入力した後、ステップＳＦ２へ進む。ステップＳＦ２では、メッセージダイジェスト作成・取得部２０５ａは、送信者（端末１００）の公開鍵を用いて送信内容確認情報１４を復号化することにより、メッセージダイジェストを作成（取得）する。

【００４５】そして、ステップＳＦ３では、電子署名確認部２０５ｃは、送信者（端末１００）の公開鍵を用いて、送信内容確認情報１４が送信者により署名されたものであるか否かを確認する。ここで、送信内容確認情報１４が送信者（端末１００）の公開鍵で復号化できた場合、送信内容確認情報１４は、送信者により署名されたものであり、一方、送信内容確認情報１４が送信者の公開鍵で復号化できなかった場合、送信内容確認情報１４

は送信者により署名されなかったものである。

【００４６】次に、ステップＳＦ４では、送信内容確認情報確認部２０５は、ステップＳＦ３の確認結果から、送信内容確認情報１４の署名が送信者（端末１００）の署名であるか否かを判断し、同判断結果が「ＮＯ」の場合、改竄もしくは通信エラーが発生したものとする。一方、ステップＳＦ４の判断結果が「ＹＥＳ」の場合、送信内容確認情報確認部２０５は、ステップＳＦ５へ進む。

【００４７】ステップＳＦ５では、送信内容確認情報１４に含まれている各種情報を分類する。ここで、上記各種情報としては、受信情報内容、前述した送信者情報、受信者情報、通信情報、メッセージダイジェスト等がある。

【００４８】また、送信内容確認情報確認部２０５は、ステップＳＦ６へ進み、受信した転送情報１１、送信者が転送した、通信に関する送信者情報、通信情報、受信者情報等を入力する。次に、ステップＳＦ７では、送信内容確認情報確認部２０５のメッセージダイジェスト作成・取得部２０５ａは、転送情報１１をハッシュ関数で圧縮して転送情報ＭＤ１２ｂ（メッセージダイジェスト）を作成する。ただし、メッセージダイジェスト作成・取得部２０５ａは、メッセージダイジェスト作成部２０２ａから転送情報ＭＤ１２ｂを取得した場合、上記作成動作を行わない。

【００４９】そして、送信内容確認情報確認部２０５は、ステップＳＦ９～ＳＦ１２で受信内容と送信内容とを比較することにより、受信内容の検証を情報毎に行う。そして、ステップＳＦ１３では、送信内容確認情報確認部２０５は、上記ステップＳＦ９～ＳＦ１２の検証結果を受けて、受信内容が送信内容と相違ないか否かを判断し、同判断結果が「ＮＯ」の場合、改竄もしくは通信エラーが発生しているものとする。一方、送信内容確認情報確認部２０５は、受信内容が送信内容と相違していない場合、ＳＦ１３の判断結果を「ＹＥＳ」として、改竄が発生していないものとする。

【００５０】以上説明したように、上述した一実施形態による情報改竄検知装置によれば、受信内容確認情報１３、送信内容確認情報１４を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

【００５１】以上本発明の実施形態について詳述してきたが、具体的な構成はこの実施形態に限定されるものではなく本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、上述した一実施形態による情報改竄検知装置においては、上述した機能を実現するための改竄検知プログラムを、フレキシブルディスク、ＣＤ－ＲＯＭ、光磁気ディスク、ＩＣカード、ＤＶＤ－ＲＯＭ等のコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録された改竄検知プログラムをコンピュータシステムに読み込ませて実行させることにより、情報の改竄検知をおこなってもよい。

【００５２】また、上記改竄検知プログラムは、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬媒体や、ハードディスク等の記憶装置等に、その全体あるいは一部が記録され、あるいは記憶されている。その改竄検知プログラムは、コンピュータにより読みとられて、動作の全部あるいは一部が実行される。また、ここでいう記録媒体は、光磁気ディスク等のように改竄検知プログラムを静的に記録しているものに限らず、インターネットの専用線、電話回線等の通信回線を通して改竄検知プログラムを送信する場合の通信回線のように、短時間の間、動的に改竄検知プログラムを保持しているもの、その場合のサーバやコンピュータ内部のメモリのように、一定時間改竄検知プログラムを保持しているものも含むものとする。

【００５３】

【発明の効果】以上説明したように、本発明によれば、受信内容確認情報、送信内容確認情報を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態による情報改竄検知装置の動作原理を説明するブロック図である。

【図２】　同一実施形態による情報改竄検知装置の構成を示すブロック図である。

【図３】　図２に示す受信内容確認情報確認部１０３の動作を説明するフローチャートである。

【図４】　図２に示す送信内容確認情報作成部１０４の動作を説明するフローチャートである。

【図５】　図２に示す受信内容確認情報作成部２０２の動作を説明するフローチャートである。

【図６】　図２に示す送信内容確認情報確認部２０５の動作を説明するフローチャートである。

【図７】　従来の情報改竄検知装置の動作原理を説明する図である。

【図８】　従来の情報改竄検知装置の欠点を説明する図である。

【符号の説明】

１００　端末
１０１　情報送信部
１０２　情報受信部
１０３　受信内容確認情報確認部
１０３ａ　メッセージダイジェスト作成部
１０３ｂ　送信者・通信・受信者情報取得部
１０３ｃ　電子署名確認部
１０４　送信内容確認情報作成部
１０４ａ　メッセージダイジェスト作成部

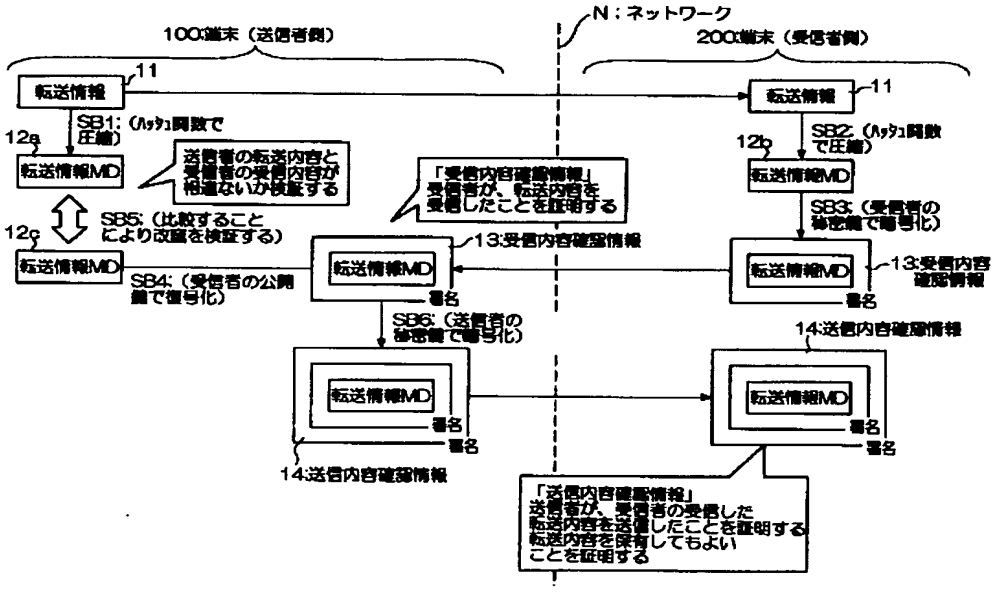
21

１０４ｂ　送信者・通信・受信者情報取得部
１０４ｃ　電子署名付加部
１０５　情報送信部
２００　端末
２０１　情報受信部
２０２　受信内容確認情報作成部
２０２ａ　メッセージダイジェスト作成部
２０２ｂ　送信者・通信・受信者情報取得部

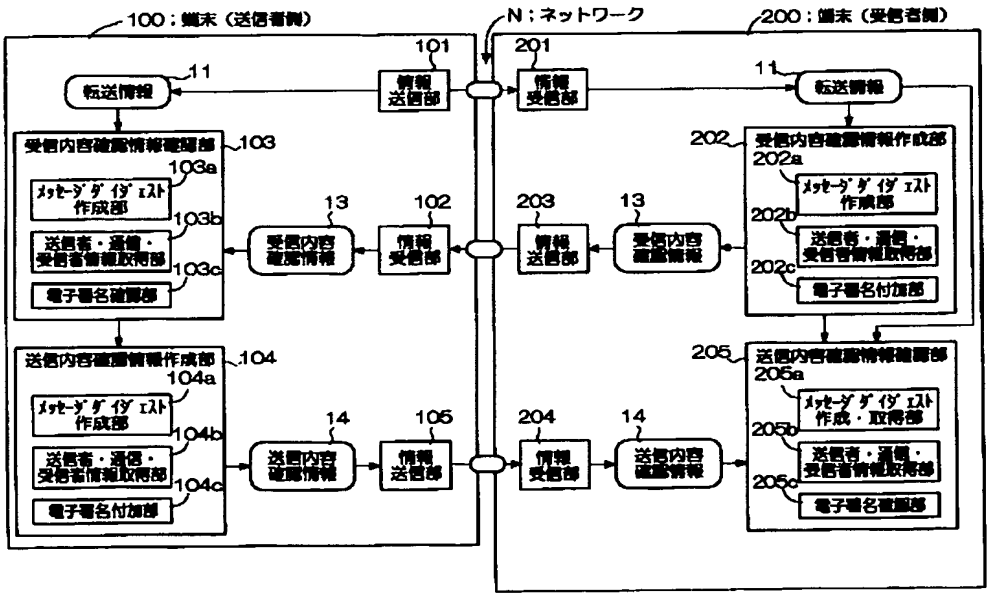
22

２０２ｃ　電子署名付加部
２０３　情報送信部
２０４　情報受信部
２０５　送信内容確認情報確認部
２０５ａ　メッセージダイジェスト作成・取得部
２０５ｂ　送信者・通信・受信者情報取得部
２０５ｃ　電子署名確認部

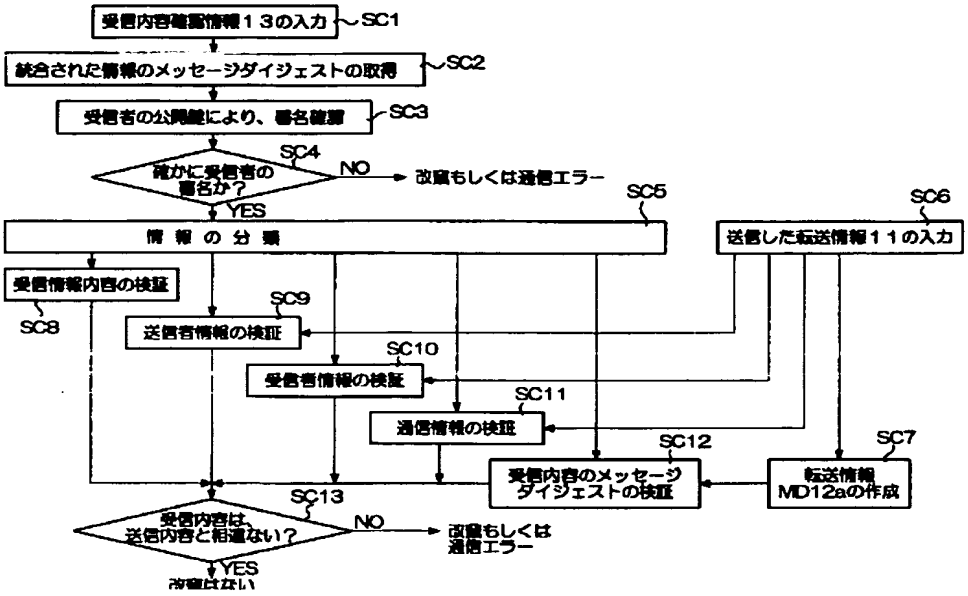
【図１】



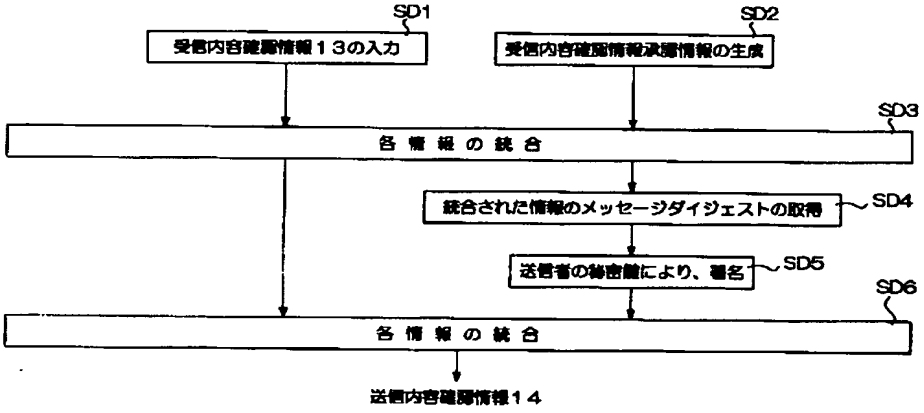
【図２】



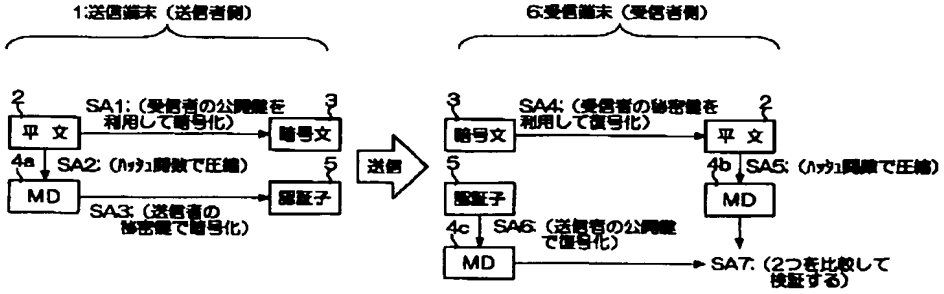
【図３】


受信内容確認情報１３の入力
SC1
統合された情報のメッセージダイジェストの取得
SC2
受信者の公開鍵により、署名確認
SC3
SC4
確かに受信者の署名か？
NO
改竄もしくは通信エラー
YES
SC5
情報の分離
SC6
送信した転送情報１１の入力
受信情報内容の検証
SC8
SC9
送信者情報の検証
SC10
受信者情報の検証
SC11
通信情報の検証
SC12
受信内容のメッセージダイジェストの検証
SC7
転送情報MD12aの作成
SC13
受信内容は、送信内容と相違ない？
NO
改竄もしくは通信エラー
YES
改竄されない

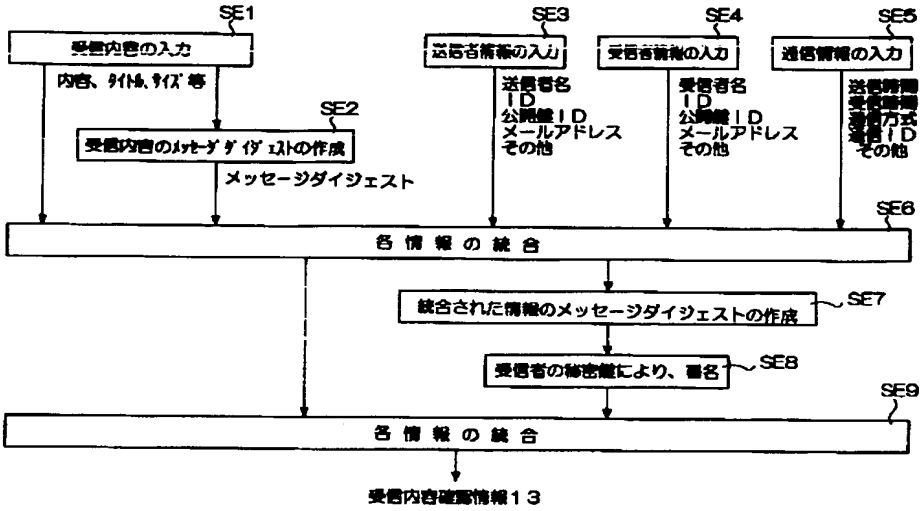
【図４】


SD1
受信内容確認情報１３の入力
SD2
受信内容確認情報承認情報の生成
SD3
各情報の統合
統合された情報のメッセージダイジェストの取得
SD4
送信者の秘密鍵により、署名
SD5
SD6
各情報の統合
送信内容確認情報１４

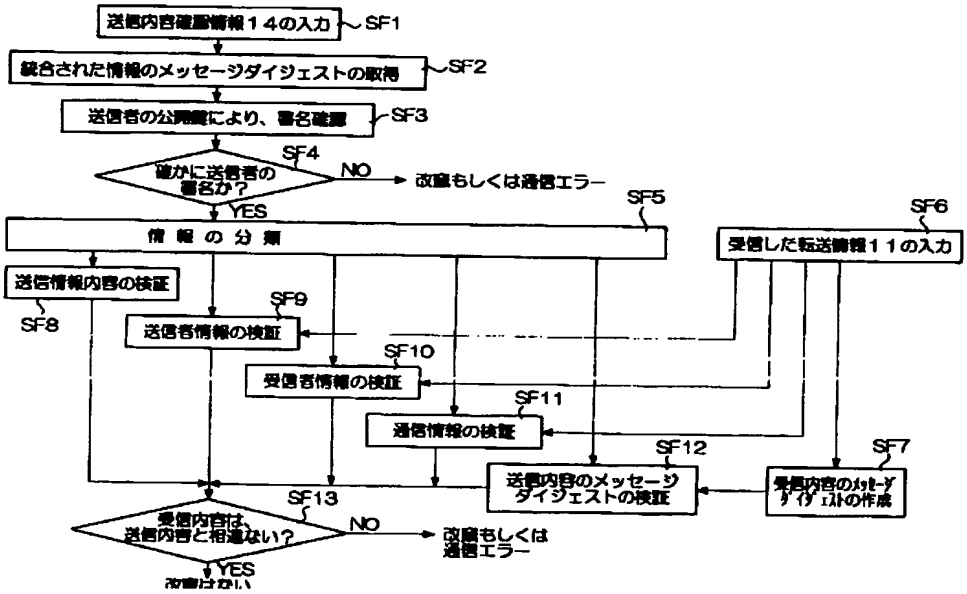
【図７】


1:送信端末（送信者側）
6:受信端末（受信者側）
2
平文
SA1:（受信者の公開鍵を利用して暗号化）
3
暗号文
4a
MD
SA2:（ハッシュ関数で圧縮）
5
署名子
SA3:（送信者の秘密鍵で暗号化）
送信
3
暗号文
SA4:（受信者の秘密鍵を利用して復号化）
2
平文
5
署名子
4b
MD
SA5:（ハッシュ関数で圧縮）
4c
MD
SA6:（送信者の公開鍵で復号化）
SA7:（2つを比較して検証する）

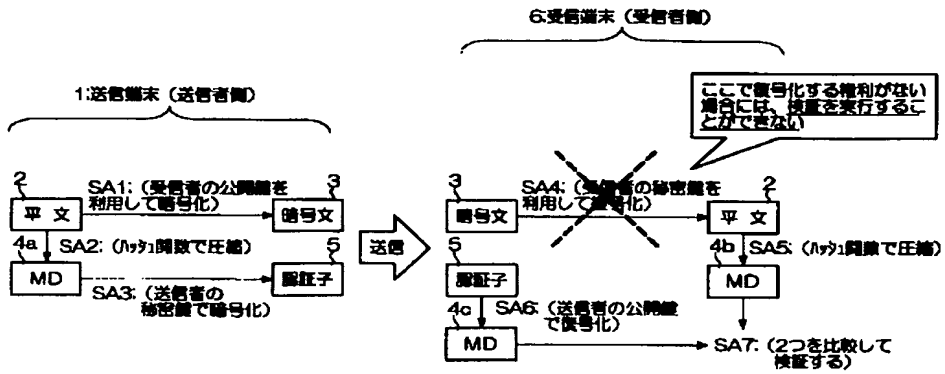
【図５】


SE1
受信内容の入力
内容、タイトル、サイズ等
SE2
受信内容のメッセージダイジェストの作成
メッセージダイジェスト
SE3
送信者情報の入力
送信者名
ID
公開鍵ID
メールアドレス
その他
SE4
受信者情報の入力
受信者名
ID
公開鍵ID
メールアドレス
その他
SE5
通信情報の入力
その他
SE6
各情報の統合
SE7
統合された情報のメッセージダイジェストの作成
SE8
受信者の秘密鍵により、署名
SE9
各情報の統合
受信内容確認情報１３

【図６】


送信内容確認情報１４の入力
SF1
統合された情報のメッセージダイジェストの取得
SF2
送信者の公開鍵により、署名確認
SF3
SF4
確かに送信者の署名か？
NO
改竄もしくは通信エラー
YES
SF5
情報の分類
SF6
受信した転送情報１１の入力
送信情報内容の検証
SF8
SF9
送信者情報の検証
SF10
受信者情報の検証
SF11
通信情報の検証
SF12
送信内容のメッセージダイジェストの検証
SF7
受信内容のメッセージダイジェストの作成
SF13
受信内容は、送信内容と相違ない？
NO
改竄もしくは通信エラー
YES

【図８】


1:送信端末（送信者側）
2
平 文
SA1:（受信者の公開鍵を利用して暗号化）
3
暗号文
4a
MD
SA2:（ハッシュ関数で圧縮）
5
署証子
SA3:（送信者の秘密鍵で暗号化）
送信
6:受信端末（受信者側）
ここで復号化する権利がない場合には、検証を実行することができない
3
暗号文
SA4:（受信者の秘密鍵を利用して復号化）
2
平 文
5
署証子
4b
SA5:（ハッシュ関数で圧縮）
MD
4c
SA6:（送信者の公開鍵で復号化）
MD
SA7:（2つを比較して検証する）